PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-331144
(43)Date of publication of application : 30.11.1999

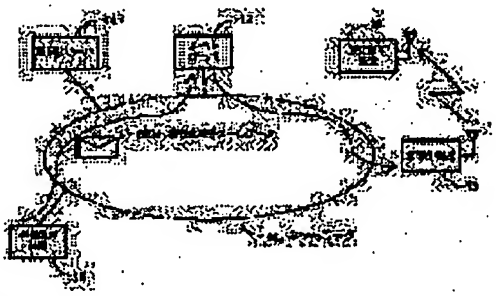
(51)Int.Cl. H04L 9/08
G06F 12/14

(21)Application number : 10-132326
(22)Date of filing : 14.05.1998

(71)Applicant : SEIKO EPSON CORP
(72)Inventor : MIYASHITA HIROBUMI
SHIMOMURA JUN
HARADA MAKOTO

(54) CIPHERING DEVICE, DECIPHERING DEVICE, PORTABLE INFORMATION PROCESSOR, CIPHERING METHOD, DECIPHERING METHOD AND PORTABLE INFORMATION PROCESSOR CONTROL METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To additionally improve the secrecy of information, without increasing the burden of a user for information control by generating a cryptographic key through the use of inputted positional information and inputted time information for ciphering inputted information through the use of the cryptographic key.
SOLUTION: In a cipher electronic mail system to be applied to a portable information processor, a ciphering server 11 generates the cryptographic key under a prescribed condition. A mail server 12 connected to a network 14 executes the processing of transferring actual ciphering electronic mail data SEM, and a radio repeating station 13 delivers an electronic mail under the control of the server 12. A transmission terminal device 15 executes the preparation of the electronic mail, request for generating a cryptographic key, ciphering processing and transmission request, and a receiving terminal device (portable information processor) 20 deciphers a received ciphered electronic mail SEM.



LEGAL STATUS

[Date of request for examination]	17.09.1999
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	3451929
[Date of registration]	18.07.2003

(19)日本国特許庁（JP）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平11－331144

(43)公開日　平成11年(1999)11月30日

(51)Int.Cl.⁶	識別記号	FI	
H04L 9/08		H04L 9/00	601B
G06F 12/14	320	G06F 12/14	320B

審査請求 有　請求項の数11 OL （全 8 頁）

(21)出願番号　特願平10－132328

(22)出願日　平成10年(1998)5月14日

(71)出願人　000002369
セイコーエプソン株式会社
東京都新宿区西新宿2丁目4番1号

(72)発明者　宮下　博文
長野県諏訪市大和3丁目3番5号　セイコーエプソン株式会社内

(72)発明者　下村　純
長野県諏訪市大和3丁目3番5号　セイコーエプソン株式会社内

(72)発明者　原田　豊
長野県諏訪市大和3丁目3番5号　セイコーエプソン株式会社内

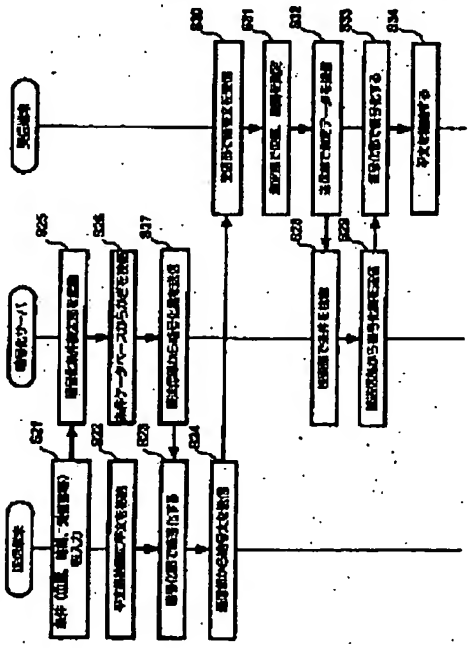
(74)代理人　弁理士　川▲崎▼　研二　（外1名）

(54)【発明の名称】　暗号化装置、復号化装置、携帯情報処理装置、暗号化方法、復号化方法及び携帯情報処理装置の制御方法

(57)【要約】

【課題】　情報管理のためのユーザの負担を増加させることなく、より情報の機密性を高める。

【解決手段】　少なくとも位置情報及び時間情報を用いて暗号化を行うことにより情報の盗難や盗聴に対する保護を高め機密性を高めることが可能となる。また、位置情報及び時間情報を自動的に取得することにより、情報管理のためのユーザの負担を増加させることもない。さらに、一つの装置が指定された時間に複数箇所で、解読処理を試みることは物理的に不可能であるため、情報が解読される確率をより低くすることができる。



1

【特許請求の範囲】

【請求項1】 入力された位置情報及び入力された時刻情報を用いて、暗号化鍵を生成する暗号化鍵生成手段と、

前記暗号化鍵を用いて入力情報を暗号化する暗号化手段と、を備えたことを特徴とする暗号化装置。

【請求項2】 請求項1記載の暗号化装置において、

前記暗号化鍵生成手段は、前記位置情報及び前記時刻情報に加えて前記入力情報の送信先を特定するための送信先特定情報を用いて前記暗号化鍵を生成することを特徴とする暗号化装置。

【請求項3】 入力された現在位置情報及び入力された現在時刻情報を用いて復号化鍵を生成する復号化鍵生成手段と、

前記復号化鍵を用いて入力暗号化情報を復号化する復号化手段と、を備えたことを特徴とする復号化装置。

【請求項4】 請求項3記載の復号化装置において、

前記復号化鍵生成手段は、前記現在位置情報及び前記現在時刻情報に加えて前記入力暗号化情報の送信先を特定するための送信先特定情報を用いて前記復号化鍵を生成することを特徴とする復号化装置。

【請求項5】 入力された暗号化データである入力暗号化情報を復号化する携帯情報処理装置において、

自己の現在位置を検出し現在位置情報を出力する自己位置検出手段と、

現在時刻を検出し現在時刻情報を出力する現在時刻検出手段と、

前記現在位置情報及び前記現在時刻情報を用いて復号化鍵を生成する復号化鍵生成手段と、

前記復号化鍵を用いて入力暗号化情報を復号化する復号化手段と、を備えたことを特徴とする携帯情報処理装置。

【請求項6】 入力された位置情報及び入力された時刻情報を用いて、暗号化鍵を生成する暗号化鍵生成処理回路と、

前記暗号化鍵を用いて入力情報を暗号化する暗号化処理回路と、を備えたことを特徴とする暗号化装置。

【請求項7】 入力された現在位置情報及び入力された現在時刻情報を用いて復号化鍵を生成する復号化鍵生成処理回路と、

前記復号化鍵を用いて入力暗号化情報を復号化する復号化処理回路と、を備えたことを特徴とする暗号化装置。

【請求項8】 入力された暗号化データである入力暗号化情報を復号化する携帯情報処理装置において、

自己の現在位置を検出し現在位置情報を出力する自己位置検出装置と、

現在時刻を検出し現在時刻情報を出力する現在時刻検出装置と、

前記現在位置情報及び前記現在時刻情報を用いて復号化鍵を生成する復号化鍵生成処理回路と、

2

前記復号化鍵を用いて入力暗号化情報を復号化する復号化処理回路と、を備えたことを特徴とする携帯情報処理装置。

【請求項9】 入力された位置情報及び入力された時刻情報を用いて、暗号化鍵を生成する暗号化鍵生成工程と、

前記暗号化鍵を用いて入力情報を暗号化する暗号化工程と、を備えたことを特徴とする暗号化方法。

【請求項10】 入力された現在位置情報及び入力された現在時刻情報を用いて復号化鍵を生成する復号化鍵生成工程と、

前記復号化鍵を用いて入力暗号化情報を復号化する復号化工程と、を備えたことを特徴とする復号化方法。

【請求項11】 入力された暗号化データである入力暗号化情報を復号化する携帯情報処理装置の制御方法において、

自己の現在位置を検出する自己位置検出工程と、

現在時刻を検出する現在時刻検出工程と、

検出した前記現在位置及び検出した前記現在時刻を用いて復号化鍵を生成する復号化鍵生成工程と、

生成した前記復号化鍵を用いて入力された暗号化情報を復号化する復号化工程と、を備えたことを特徴とする携帯情報処理装置の制御方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、暗号化装置、復号化装置、携帯情報処理装置、暗号化方法、復号化方法及び携帯情報処理装置の制御方法に係り、特に情報セキュリティを確保する技術に関する。

【0002】

【従来の技術】近年、インターネットやパーソナルコンピュータ通信ネットワーク等のネットワークを介して複数の情報処理装置が接続され、このネットワークを介して情報のやりとりが行われている。ところで、送信者から受信者にネットワークを介して送信される情報や、ネットワークに接続されたコンピュータに格納されている情報は、従来の書類などに記載されている情報と比較してより盗聴される可能性が高い。

【0003】そこで、特開平9-319662号公報記載の情報処理装置においては、GPS測量によって自己の現在位置を取得する位置取得部を備え、特定情報（ファイル）にアクセスする際には、情報管理部が位置取得部により取得した現在位置（パスワード情報あるいはキー情報に相当）を特定情報に対応する所在地情報と照合し、現在位置と所在地情報に対応する位置とが合致している場合にのみ、特定情報の復号化を行い、表示等を行う構成が開示され、所在地情報に対応する位置以外では特定情報にアクセスすることができなくなり、ユーザがパスワード情報あるいはキー情報を管理（記憶及び入力）する手間を削減しつつ、特定情報の盗難や盗聴に対

3

し、特定情報を保護することができる旨が記載されている。

【0004】

【発明が解決しようとする課題】上記従来の情報処理装置においては、現在位置をパスワード情報あるいはキー情報として用いているため、例えば、現在位置（場所）を変更しながら、特定情報にアクセスすることにより、アクセスできてしまう可能性があった。そこで、本発明の目的は、情報管理のためのユーザの負担を増加させることなく、より情報の機密性を高めることが可能な情報処理装置及び情報処理方法を提供することにある。

【0005】

【課題を解決するための手段】上記課題を解決するため、請求項1記載の構成は、入力された位置情報及び入力された時刻情報を用いて、暗号化鍵を生成する暗号化鍵生成手段と、前記暗号化鍵を用いて入力情報を暗号化する暗号化手段と、を備えたことを特徴としている。

【0006】請求項2記載の構成は、請求項1記載の構成において、前記暗号化鍵生成手段は、前記位置情報及び前記時刻情報に加えて前記入力情報の送信先を特定するための送信先特定情報を用いて前記暗号化鍵を生成することを特徴としている。

【0007】請求項3記載の構成は、入力された現在位置情報及び入力された現在時刻情報を用いて復号化鍵を生成する復号化鍵生成手段と、前記復号化鍵を用いて入力暗号化情報を復号化する復号化手段と、を備えたことを特徴としている。

【0008】請求項4記載の構成は、請求項3記載の構成において、前記復号化鍵生成手段は、前記現在位置情報及び前記現在時刻情報に加えて前記入力暗号化情報の送信先を特定するための送信先特定情報を用いて前記復号化鍵を生成することを特徴としている。

【0009】請求項5記載の構成は、入力された暗号化データである入力暗号化情報を復号化する携帯情報処理装置において、自己の現在位置を検出し現在位置情報を出力する自己位置検出手段と、現在時刻を検出し現在時刻情報を出力する現在時刻検出手段と、前記現在位置情報及び前記現在時刻情報を用いて復号化鍵を生成する復号化鍵生成手段と、前記復号化鍵を用いて入力暗号化情報を復号化する復号化手段と、を備えたことを特徴としている。

【0010】請求項6記載の構成は、入力された位置情報及び入力された時刻情報を用いて、暗号化鍵を生成する暗号化鍵生成処理回路と、前記暗号化鍵を用いて入力情報を暗号化する暗号化処理回路と、を備えたことを特徴としている。

【0011】請求項7記載の構成は、入力された現在位置情報及び入力された現在時刻情報を用いて復号化鍵を生成する復号化鍵生成処理回路と、前記復号化鍵を用いて入力暗号化情報を復号化する復号化処理回路と、を備えたことを特徴としている。

4

【0012】請求項8記載の構成は、入力された暗号化データである入力暗号化情報を復号化する携帯情報処理装置において、自己の現在位置を検出し現在位置情報を出力する自己位置検出装置と、現在時刻を検出し現在時刻情報を出力する現在時刻検出装置と、前記現在位置情報及び前記現在時刻情報を用いて復号化鍵を生成する復号化鍵生成処理回路と、前記復号化鍵を用いて入力暗号化情報を復号化する復号化処理回路と、を備えたことを特徴としている。

【0013】請求項9記載の構成は、入力された位置情報及び入力された時刻情報を用いて、暗号化鍵を生成する暗号化鍵生成工程と、前記暗号化鍵を用いて入力情報を暗号化する暗号化工程と、を備えたことを特徴としている。

【0014】請求項10記載の構成は、入力された現在位置情報及び入力された現在時刻情報を用いて復号化鍵を生成する復号化鍵生成工程と、前記復号化鍵を用いて入力暗号化情報を復号化する復号化工程と、を備えたことを特徴としている。

【0015】請求項11記載の構成は、入力された暗号化データである入力暗号化情報を復号化する携帯情報処理装置の制御方法において、自己の現在位置を検出する自己位置検出工程と、現在時刻を検出する現在時刻検出工程と、検出した前記現在位置及び検出した前記現在時刻を用いて復号化鍵を生成する復号化鍵生成工程と、生成した前記復号化鍵を用いて入力された暗号化情報を復号化する復号化工程と、を備えたことを特徴としている。

【0016】

【発明の実施の形態】つぎに図面を参照して本発明の好適な実施形態について説明する。

（1） 暗号電子メールシステムの構成

図1に実施形態の携帯情報処理装置が適用される暗号電子メールシステムを構築した場合の概要構成図を示す。暗号電子メールシステム10は、所定条件の下で暗号鍵の生成を行う暗号化サーバ11、実際の暗号化電子メールデータSEMを転送する処理を行うメールサーバ12及びメールサーバ12の制御下で電子メールを配信する無線中継局13が接続されたネットワーク14と、ネットワーク14に接続され、電子メールの作成、暗号鍵生成依頼、暗号化処理及び送信依頼を行う情報処理装置（以下、送信端末装置という）15と、受信した暗号化電子メールSEMの復号化を行う携帯情報処理装置（以下、受信端末装置という）20と、を備えて構成されている。

【0017】（2） 受信端末装置の構成

図2に実施形態の受信端末装置の概要構成ブロック図を示す。受信端末装置20は、移動通信端末装置を制御するCPU21と、各種データを記憶するメモリ（ROM

及びRAM）２２と、各種データを表示するための液晶ディスプレイなどで構成された表示装置２８と、各種情報を入力するためのキーボード、タッチパネルなどで構成された入力装置２４と、各種データを記憶するためのハードディスクドライブ（HDD）、フレキシブルディスクドライブ（FDD）などの外部記憶装置２５と、通信機器用アンテナ２６を介して図示しない無線基地局との間で無線通信を行うためのデータ通信装置２７と、GPSアンテナ２８を介してGPS衛星からの電波を受信するGPS受信機２９と、GPS受信機２９の出力信号に基づいて受信端末装置２０の現在位置データを演算し、現在時刻データを抽出して出力するGPS用計算機３０と、各種音声出力を行うスピーカ３１と、各種拡張用機器を接続するための拡張バスインターフェース装置３２と、受信端末装置２０を構成する各装置２１～３２を接続するための内部バス３３と、を備えて構成されている。

【００１８】（３） 暗号電子メールシステムの動作

つぎに図３の暗号システムの機能構成ブロック図及び図４の処理シーケンス図を参照して暗号電子メールシステムの動作について説明する。

（３．１） 条件データベース部の構成

ここで、暗号電子メールシステムの動作説明に先立ち、条件データベース部４１（図３参照）のデータ構成例について説明する。なお、暗号化鍵と復号化鍵の構成は同様の構成のため、以下の説明においては、暗号化鍵についてのみ説明する。

【００１９】条件データベース部４１は、例えば、図５に示すように、位置テーブル４１P、時間テーブル４１T及びユーザ特定テーブル４２Uを備えている。位置テーブル４１Pは、位置に対応づけて位置暗号化鍵を格納している。例えば、位置Bに対応する位置暗号化鍵はBとなる。この場合において、位置情報としては、緯度範囲、経度範囲などの位置座標や、第１会議室、第２応接室などの部屋単位等により設定することが可能である。

【００２０】また、時間テーブル４１Tは、時間に対応づけて時間暗号化鍵を格納している。例えば、時間Dに対応する時間暗号化鍵はD'となる。この場合において、時間情報としては、○○時～○○時、□日、△曜日等の単位で設定することが可能である。また、ユーザ特定テーブル４２Uは、ユーザに対応づけてユーザ特定暗号化鍵を格納している。例えば、ユーザFに対応するユーザ特定暗号化鍵はF"となる。この場合において、ユーザ特定情報としては、○○さん、□□チーム、△△課等の単位で設定することが可能である。

【００２１】これらの位置暗号化鍵及び時間暗号鍵は本実施形態では、必須であるが、ユーザ特定暗号化鍵は、必要に応じて用いればよい。これに対応して、ユーザ特定復号化鍵も必要に応じて用いればよい。以下の説明においては、一組の位置暗号化鍵及び時間暗号化鍵あるいは一組の位置暗号化鍵、時間暗号化鍵及びユーザ特定暗号化鍵を暗号化鍵と総称し、一組の位置復号化鍵及び時間復号化鍵あるいは一組の位置復号化鍵、時間復号化鍵及びユーザ特定復号化鍵を復号化鍵と総称している。

【００２２】（３．２） 暗号電子メールシステムの具体的動作

つぎに動作を説明する。まず、送信端末装置１５の暗号化条件設定部３１は、暗号化サーバ１１に対して暗号化条件を設定する（ステップS１、S２１）より具体的には、例えば、暗号化条件として、少なくとも、受信場所及び受信時間を設定し、必要に応じて受信者を設定する。これにより暗号化サーバ１１は、暗号化条件設定部４１を起動し（ステップS２５）、暗号化条件設定部４１は、設定された暗号化条件に従って、条件データベース部４２から暗号化鍵を検索し（ステップS２、S２６）、鍵送信部４７に出力させる（ステップS３）。

【００２３】これにより鍵送信部４７は、検索された暗号化鍵を送信端末装置１５の暗号化部３３に送信する（ステップS４、S２７）。これと並行して送信端末装置１５は、平文格納部３２に用意された電子メールの平文を格納する（ステップS２２）。そして、送信端末装置１５の暗号化部３３は、平文格納部３２から電子メールの平文を読み出し（ステップS５）、電子メールの暗号化を行い、暗号化電子メールデータSEMを生成し（ステップS２７）、通信部３４に出力する（ステップS６）。

【００２４】これにより送信端末装置１５の通信部３４は、入力された暗号化電子メールデータSEMを受信端末装置２０に対して送信する（ステップS７、S２４）。より具体的には、送信端末装置１５の通信部３４は、ネットワーク１４を介して暗号化電子メールデータSEMをメールサーバ１２に送信する。この結果、メールサーバ１２は、受信した暗号化電子メールデータSEMを格納し、保持することとなる。

【００２５】そして、メールサーバ１２に対し、受信端末装置２０から暗号化電子メールデータの転送が要求されると、メールサーバ１２は、無線中継局１３及び無線回線を介して受信端末装置２０に送信することとなる。受信端末装置２０の受信部４５は、送信された暗号化電子メールデータSEMを受信し（ステップS３０）、暗号文格納部４６に格納する（ステップS８）。より具体的には、受信部４５として機能する通信機器用アンテナ２６及びデータ通信装置１７は、送信された暗号化電子メールデータSEMを暗号文格納部４６として機能する外部記憶装置２５内に格納する。

【００２６】そして、受信端末装置２０のユーザにより暗号化電子メールデータSEMの復号化が指示されると、受信端末装置２０の測定部４７は、自己の現在位置及び現在時刻を測定して（ステップS３１）、送信部４８に出力する（ステップS９）。これにより、送信部４

８は、暗号化サーバ１１にアクセスし、現在位置情報及び現在時刻情報を測定データとして暗号化サーバ１１の検索部４４に送信する（ステップＳ１０、Ｓ３２）。より具体的には、ＧＰＳ受信機２９及びＧＰＳ用計算機３０が測定部４７として機能し、ＧＰＳ受信機２９がＧＰＳアンテナ２８を介してＧＰＳ衛星からの電波を受信してＧＰＳ用計算機３０に出力する。

【００２７】ＧＰＳ用計算機３０は、ＧＰＳ受信機２９の出力信号に基づいて受信端末装置２０の現在位置データを演算し、現在時刻データを抽出して測定データとしてデータ通信装置２７及びメモリ２２に出力する。これにより通信部４８として機能するデータ通信装置２７は、通信機用アンテナ２６を介して暗号化サーバ１１に現在位置データ及び現在時刻データを送信することとなる。暗号化サーバ１１の検索部４４は、条件データベース部４２から復号化鍵を検索し（ステップＳ１１、Ｓ２８）、鍵送信部４７に出力させる（ステップＳ１２）。

【００２８】鍵送信部４７は、検索された復号化鍵を送信端末装置１５の復号化部５０に送信する（ステップＳ１３、Ｓ２９）。これにより復号化部５０は、暗号文格納部４６から暗号化電子メールデータＳＥＭを読み出すとともに、当該受信端末装置２０のユーザを特定するための秘密鍵が予め格納された秘密鍵格納部４９から秘密鍵を読み出す（ステップＳ１４、Ｓ１５）。

【００２９】そして復号化部５０は、送信された復号化鍵及び秘密鍵を用いて暗号化電子メールデータＳＥＭの復号化し（ステップＳ３３）、電子メールデータの平文を平文格納部５１であるメモリ２２あるいは外部記憶装置２５に格納する（ステップＳ１６、Ｓ３４）。この結果、ＣＰＵ２１は、電子メールデータの平文を表示装置２３に表示することができ、ユーザは電子メールの内容を読むことが可能となる。

【００３０】（４）　実施形態の効果

以上の説明のように本実施形態によれば、少なくとも位置（場所）及び時間を使用して暗号化を行うことにより情報の盗難や盗聴に対する保護を高めることができる。すなわち、特定の時刻に特定の場所に行かなければ受信した情報を復号化することができないので、例えば、機密性の高い情報をある特定の場所まで漏洩することなく保護しておくことが可能となる。

【００３１】しかも、位置（現在位置）や時間（現在時刻）は自動的に取得されるため、ユーザの情報管理は必要でなくなり、手間を簡略化することができる。また、特定の受信端末装置が指定された時間に複数箇所で、解読処理を行うことは物理的に不可能であり、情報が解読される確率をより低くすることができる。

【００３２】（５）　実施形態の変形例

以上の説明においては、暗号化鍵として、位置暗号化鍵、時間暗号化鍵、ユーザ特定暗号化鍵を用いていたが、さらに任意の暗号化鍵や任意のパスワードを組み合わせることも可能である。上記説明においては、位置情報及び時間情報を暗号化鍵として用いる場合について説明したが、これらの一方または双方をパスワードとして処理を行うように構成したり、パスワード及び暗号化鍵として処理を行うように構成することも可能である。

【００３３】また、上記説明においては、自己位置検出手段として、ＧＰＳ衛星を使ったＧＰＳを利用していたが、適当に設置した疑似ＧＰＳ衛星（ＧＰＳ電波発信機）による疑似ＧＰＳ情報や、ＰＨＳなどにおける位置登録情報を用いたり、構内ＰＨＳ等のように、無線基地局を特定する情報を利用するように構成することも可能である。これにより、複数無線ゾーン単位や部屋単位で自己位置を検出することができる。

【００３４】また、暗号化方式としては、共通鍵方式または公開鍵方式のいずれの方式であっても構わない。例えば、共通鍵方式の場合には、上述した位置暗号化鍵（必須）、時間暗号化鍵（任意）、送信者の公開鍵及び受信者のＥメールアドレスを所定の演算により組み合わせることにより共通鍵を生成することができる。以上の説明においては、電子メールシステムの場合について説明したが、電子メールデータに限らず、電子化可能なデータであれば、適用が可能である。例えば、極秘データについては、社内の特定の場所でなければ、閲覧等できないようにすることにより、権限のない社員によるデータの読み出し等を防止することができる。

【００３５】

【発明の効果】本発明によれば、少なくとも位置情報及び時間情報を用いて暗号化を行うことにより情報の盗難や盗聴に対する保護を高め機密性を高めることが可能となる。また、位置情報及び時間情報を自動的に取得することにより、情報管理のためのユーザの負担を増加させることもない。さらに、一つの装置が指定された時間に複数箇所で、解読処理を試みることは物理的に不可能であるため、情報が解読される確率をより低くすることができる。

【図面の簡単な説明】

【図１】　暗号電子メールシステムを構築した場合の概要構成図である。

【図２】　受信端末装置の概要構成ブロック図である。

【図３】　暗号電子メールシステムの機能構成ブロック図である。

【図４】　暗号電子メールシステムの処理シーケンス図である。

【図５】　条件データベース部におけるデータ構成例について説明する図である。

【符号の説明】

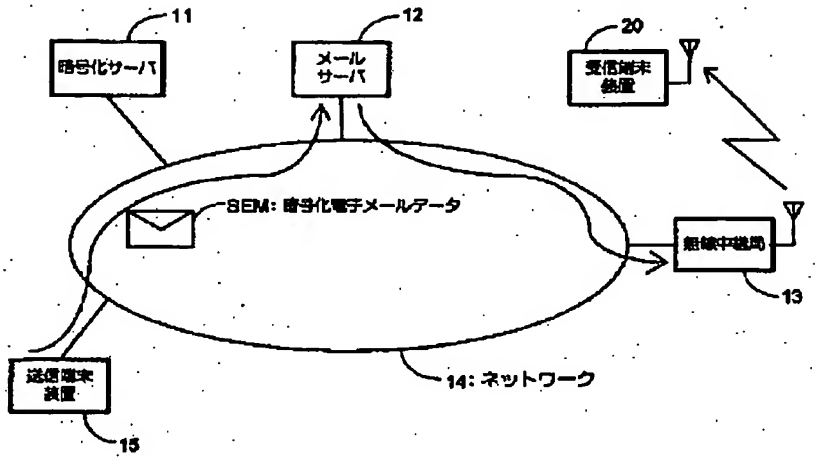
１０…暗号電子メールシステム、

１１…暗号化サーバ、

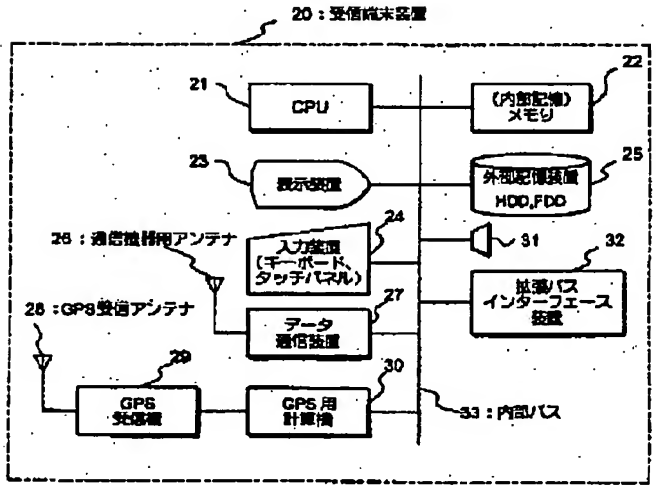
１２…メールサーバ、

１３…無線中継局、
１４…ネットワーク、
１５…送信端末装置、
２０…受信端末装置（携帯型情報処理装置）、
２１…ＣＰＵ、
２２…メモリ、
２３…表示装置、
２４…入力装置、
２５…外部記憶装置、
２６…通信機用アンテナ、
２７…データ通信装置、
２８…ＧＰＳ受信アンテナ、
２９…ＧＰＳ受信機、
３０…ＧＰＳ用計算機、
３１…スピーカ、
３２…拡張バスインターフェース、
３３…内部バス

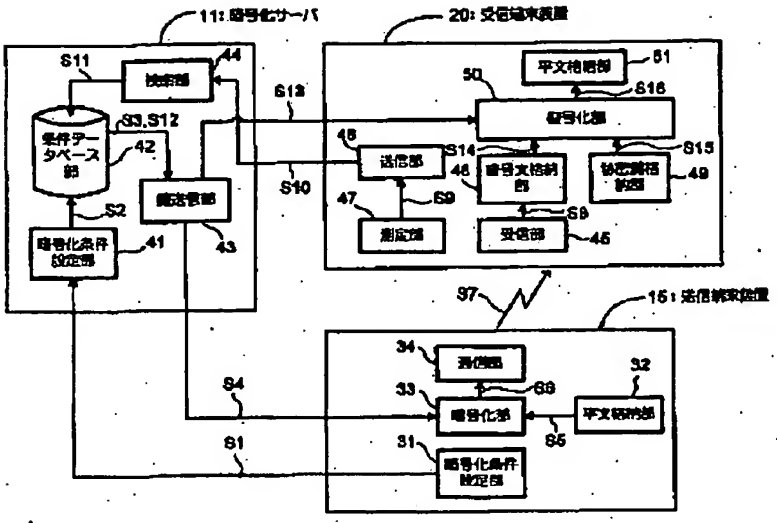
【図１】



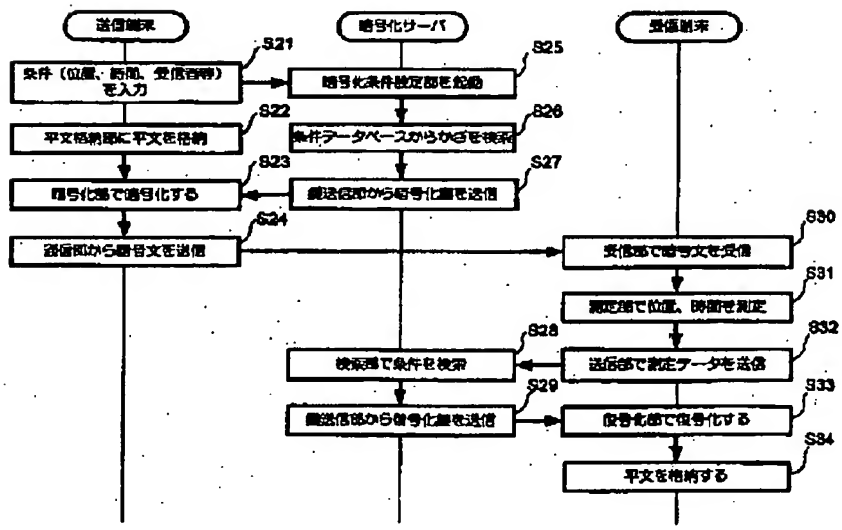
【図２】



【図3】


11:暗号化サーバ
20:受信端末装置
S11
44
検索部
S12
S3,S12
条件データベース部
42
S2
暗号化条件設定部
41
43
S10
S4
S1
45
送信部
S14
暗号文格納部
46
S15
秘密鍵情報部
49
47
S9
測定部
S8
受信部
45
97
15:送信端末装置
34
通信部
S6
33
暗号化部
S5
32
平文格納部
31
暗号化条件設定部

【図4】


送信端末
暗号化サーバ
受信端末
S21
条件（位置、時間、受信者等）を入力
S25
暗号化条件設定部を起動
S22
平文格納部に平文を格納
S26
条件データベースからかぎを検索
S23
暗号化部で暗号化する
S27
最適信局から暗号化鍵を送信
S24
送信局から暗号文を送信
S30
受信部で暗号文を受信
S31
測定部で位置、時間を測定
S28
検索部で条件を検索
S32
送信部で測定データを送信
S29
最適信局から暗号化鍵を送信
S33
復号化部で復号化する
S34
平文を格納する

【図5】

(a) 位置テーブル

位置 A	位置暗号化鍵 A
位置 B	位置暗号化鍵 B
位置 C	位置暗号化鍵 C
位置 D	位置暗号化鍵 D
位置 E	位置暗号化鍵 E
位置 F	位置暗号化鍵 F

(b) 時間テーブル

時間 A	時間暗号化鍵 A'
時間 B	時間暗号化鍵 B'
時間 C	時間暗号化鍵 C'
時間 D	時間暗号化鍵 D'
時間 E	時間暗号化鍵 E'
時間 F	時間暗号化鍵 F'

(c) ユーザ特定テーブル

ユーザA	ユーザ特定暗号化鍵 A"
ユーザB	ユーザ特定暗号化鍵 B"
ユーザC	ユーザ特定暗号化鍵 C"
ユーザD	ユーザ特定暗号化鍵 D"
ユーザE	ユーザ特定暗号化鍵 E"
ユーザF	ユーザ特定暗号化鍵 F"

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[The technical field to which invention belongs] This invention relates to the technology of starting encryption equipment, decryption equipment, a pocket information processor, the encryption method, the decryption method, and the control method of a pocket information processor, especially securing an information security.
[0002]
[Description of the Prior Art] In recent years, two or more information processors are connected through networks, such as the Internet and a personal computer communication network, and the informational exchange is performed through this network. By the way, the information transmitted to an addressee through a network from a transmitting person and the information stored in the computer connected to the network have a high possibility of being intercepted more as compared with the information indicated by the conventional document etc.
[0003] Then, it sets to an information processor given in JP,9-319662,A. In case it has the location acquisition section which acquires the self current position and specific information (file) is accessed by GPS location survey The current position (equivalent to password information or key information) which the Research and Data Processing Department acquired by the location acquisition section is collated with the address information corresponding to specific information. Only when the current position and the location corresponding to address information have agreed Decrypt specific information, the configuration which performs a display etc. is indicated, and it becomes impossible to access specific information except the location corresponding to address information. The purport from which specific information can be protected is indicated to the theft of specific information, or tapping, reducing the time and effort to which a user manages password information or key information (storage and input).
[0004]
[Problem(s) to be Solved by the Invention] In the above-mentioned conventional information processor, it may be able to access by accessing specific information, changing the current position (location), since the current position is used as password information or key information. Then, the purpose of this invention is to offer the information processor which can raise informational confidentiality more, and the information processing method, without making the burden of the user for information management increase.
[0005]
[Means for Solving the Problem] In order to solve the above-mentioned technical problem, a configuration according to claim 1 is characterized by having an encryption key generation means to generate an encryption key, and an encryption means to encipher input using said encryption key, using inputted positional information and inputted time information.
[0006] A configuration according to claim 2 is characterized by said encryption key generation means generating said encryption key using transmission place specific information for specifying a transmission place of said input in addition to said positional information and said time information in a configuration according to claim 1.
[0007] A configuration according to claim 3 is characterized by having a decryption key

generation means to generate a decryption key using inputted currency information and inputted current time information, and a decryption means to decrypt input encryption information using said decryption key.

[0008] A configuration according to claim 4 is characterized by said decryption key generation means generating said decryption key using transmission place specific information for specifying a transmission place of said input encryption information in addition to said currency information and said current time information in a configuration according to claim 3.

[0009] In a pocket information processor which decrypts input encryption information that a configuration according to claim 5 is inputted encryption data A self-location detection means to detect the self current position and to output currency information, It is characterized by having a current time detection means to detect current time and to output current time information, a decryption key generation means to generate a decryption key using said currency information and said current time information, and a decryption means to decrypt input encryption information using said decryption key.

[0010] A configuration according to claim 6 is characterized by having an encryption key generation processing circuit which generates an encryption key, and an encryption processing circuit which enciphers input using said encryption key using inputted positional information and inputted time information.

[0011] A configuration according to claim 7 is characterized by having a decryption key generation processing circuit which generates a decryption key using inputted currency information and inputted current time information, and a decryption processing circuit which decrypts input encryption information using said decryption key.

[0012] In a pocket information processor which decrypts input encryption information that a configuration according to claim 8 is inputted encryption data Self-location detection equipment which detects the self current position and outputs currency information, It is characterized by having current time detection equipment which detects current time and outputs current time information, a decryption key generation processing circuit which generates a decryption key using said currency information and said current time information, and a decryption processing circuit which decrypts input encryption information using said decryption key.

[0013] A configuration according to claim 9 is characterized by having an encryption key generation production process which generates an encryption key, and an encryption production process which enciphers input using said encryption key using inputted positional information and inputted time information.

[0014] A configuration according to claim 10 is characterized by having a decryption key generation production process which generates a decryption key using inputted currency information and inputted current time information, and a decryption production process which decrypts input encryption information using said decryption key.

[0015] In a control method of a pocket information processor which decrypts input encryption information that a configuration according to claim 11 is inputted encryption data A self-location detection production process of detecting the self current position, and a current time detection production process of detecting current time, It is characterized by having a decryption key generation production process which generates a decryption key using said detected current position and said detected current time, and a decryption production process which decrypts encryption information inputted using said generated decryption key.

[0016]

[Embodiment of the Invention] With reference to a drawing, the suitable operation gestalt of this invention is explained below.

(1) The outline block diagram at the time of building the code electronic mail system with which the pocket information processor of an operation gestalt is applied to the block diagram 1 of a code electronic mail system is shown. The code electronic mail system 10 The network 14 where the radio relay station 13 which distributes an electronic mail under control of the encryption server 11 which generates a cryptographic key under predetermined conditions, the mail server 12 which performs processing which transmits the actual encryption electronic mail data SEM, and a mail server 12 was connected, The information processor 15 which is connected to a

network 14 and performs creation of an electronic mail, a cryptographic key generation request, encryption processing, and a transmitting request (henceforth transmit-terminal equipment), It has the pocket information processor (henceforth accepting-station equipment) 20 which decrypts encryption electronic mail SEM which received, and is constituted.

[0017] (2) Outline configuration block drawing of the accepting-station equipment of an operation gestalt is shown in the block diagram 2 of accepting-station equipment. CPU21 by which accepting-station equipment 20 controls a migration communication terminal, and the memory 22 which memorizes various data (ROM and RAM), The display 23 which consisted of liquid crystal displays for displaying various data etc., The input unit 24 which consisted of a keyboard for inputting various information, a touch panel, etc., The external storage 25, such as a hard disk drive (HDD) for memorizing various data, and a flexible disk drive (FDD), with the data communication unit 27 for performing radio communications between the base transceiver stations which are not a drawing example through the antenna 26 for communication equipment GPS receiver 29 which receives the electric wave from a GPS Satellite through the GPS antenna 28, The computer 30 for GPS which calculates the current position data of accepting-station equipment 20 based on the output signal of GPS receiver 29, and extracts and outputs current time data, It has the internal bus 33 for connecting each equipments 21-32 which constitute the expansion bus interface device 32 and the accepting-station equipment 20 for connecting the various devices for an escape with the loudspeaker 31 which performs various voice outputs, and is constituted.

[0018] (3) actuation of a code electronic mail system — explain actuation of a code electronic mail system below with reference to functional configuration block drawing of the code system of drawing 3 , and the processing sequence diagram of drawing 4 .

(3.1) the configuration of the condition data base section — here, explain the example of a data configuration of the condition data base section 41 (refer to drawing 3) in advance of explanation of a code electronic mail system of operation. In addition, the configuration of an encryption key and a decryption key explains only an encryption key in the following explanation for the same configuration.

[0019] The condition data base section 41 is equipped with location table 41P, time amount table 41T, and user specification table 42U as shown in drawing 5 . Location table 41P are matched with a location, and store the location encryption key. For example, the location encryption key corresponding to a location B is set to B. In this case, as positional information, it is possible to set up by room units, such as a position coordinate of a LAT range, a LONG range, etc., and the 1st conference room, the 2nd drawing room, etc.

[0020] Moreover, time amount table 41T are matched with time amount, and store the time amount encryption key. For example, the time amount encryption key corresponding to time amount D becomes D'. In this case, as a hour entry, it is possible at the time of the time of OO - OO to set up in units, such as ** day and ** day of the week. Moreover, user specification table 42U is matched with a user, and stores the user specification encryption key. For example, the user specification encryption key corresponding to User F becomes F." In this case, as user specific information, it is possible to set up in units, such as Mr. OO, **** team, and **** division.

[0021] What is necessary is just to use a user specification encryption key if needed, although these location encryption keys and a time amount cryptographic key are indispensable with this operation gestalt. What is necessary is just to also use a user specification decryption key if needed corresponding to this. In the following explanation, the location encryption key of a lot and the time amount encryption key or the location encryption key of a lot, the time amount encryption key, and the user specification encryption key were named the encryption key generically, and the location decryption key of a lot and the time amount decryption key or the location decryption key of a lot, the time amount decryption key, and the user specification decryption key are named the decryption key generically.

[0022] (3.2) concrete actuation of a code electronic mail system — explain actuation below. first, the encryption conditioning section 31 of transmit-terminal equipment 15 — the encryption server 11 — receiving — encryption conditions — setting up (steps S1 and S21) — as

encryption conditions, a receiving location and time of delivery are set up, and, specifically, an addressee is set up at least if needed. Thereby, the encryption server 11 starts the encryption conditioning section 41 (step S25), and the encryption conditioning section 41 searches an encryption key from the condition data base section 42 (steps S2 and S26), and it makes it output it to the key transmitting section 47 according to the set-up encryption conditions (step S3).

[0023] Thereby, the key transmitting section 47 transmits the searched encryption key to the encryption section 33 of transmit-terminal equipment 15 (step S4, S27). In parallel to this, transmit-terminal equipment 15 stores the plaintext of the electronic mail prepared for the plaintext storing section 32 (step S22). And the encryption section 33 of transmit-terminal equipment 15 reads the plaintext of an electronic mail from the plaintext storing section 32 (step S5), enciphers an electronic mail, generates the encryption electronic mail data SEM (step S27), and outputs it to the communications department 34 (step S6).

[0024] Thereby, the communications department 34 of transmit-terminal equipment 15 transmits the inputted encryption electronic mail data SEM to accepting-station equipment 20 (steps S7 and S24). More specifically, the communications department 34 of transmit-terminal equipment 15 transmits the encryption electronic mail data SEM to a mail server 12 through a network 14. Consequently, a mail server 12 will store and hold the received encryption electronic mail data SEM.

[0025] And when an encryption electronic mail data transfer is required from accepting-station equipment 20 from a mail server 12, a mail server 12 will transmit to accepting-station equipment 20 through a radio relay station 13 and a wireless circuit. The receive section 45 of accepting-station equipment 20 receives the transmitted encryption electronic mail data SEM (step S30), and stores in the cipher storing section 46 (step S8). More specifically, the antenna 26 for communication equipment and data communication unit 17 which function as a receive section 45 store the transmitted encryption electronic mail data SEM in the external storage 25 which functions as the cipher storing section 46.

[0026] And if a decryption of the encryption electronic mail data SEM is directed by the user of accepting-station equipment 20, the test section 47 of accepting-station equipment 20 will measure self current position and current time (step S31), and will output them to the transmitting section 48 (step S9). Thereby, the transmitting section 48 accesses the encryption server 11, and transmits to the retrieval section 44 of the encryption server 11 by using currency information and current time information as measurement data (steps S10 and S32). GPS receiver 29 and the computer 30 for GPS function as a test section 47, and GPS receiver 29 receives the electric wave from a GPS Satellite through the GPS antenna 28, and, more specifically, outputs to the computer 30 for GPS.

[0027] The computer 30 for GPS calculates the current position data of accepting-station equipment 20 based on the output signal of GPS receiver 29, extracts current time data, and outputs it to a data communication unit 27 and memory 22 as measurement data. the data communication unit 27 which functions as the communications department 48 by this transmits current position data and current time data to the encryption server 11 through the antenna 26 for transmitters — ** — it becomes. The retrieval section 44 of the encryption server 11 searches a decryption key from the condition data base section 42 (steps S11 and S28), and is made to output it to the key transmitting section 47 (step S12).

[0028] The key transmitting section 47 transmits the searched decryption key to the decryption section 50 of transmit-terminal equipment 15 (steps S13 and S29). Thereby, the decryption section 50 reads a private key from the private key storing section 49 in which the private key for specifying the user of the accepting-station equipment 20 concerned was stored beforehand while reading the encryption electronic mail data SEM from the cipher storing section 46 (steps S14 and S15).

[0029] And using the decryption key and private key which were transmitted, the encryption electronic mail data SEM decrypts the decryption section 50 (step S33), and it stores the plaintext of electronic mail data in the memory 22 or external storage 25 which is the plaintext storing section 51 (steps S16 and S34). Consequently, CPU21 can display the plaintext of

electronic mail data on a display 23, and becomes that a user can read the contents of the electronic mail.

[0030] (4) According to this operation gestalt, the protection to an informational theft or tapping can be raised by enciphering at least using a location (location) and time amount like explanation beyond the effect of an operation gestalt. That is, since the information received if it did not go to a specific location at specific time of day cannot be decrypted, it becomes possible to protect without, for example, revealing the high information on confidentiality to a certain specific location.

[0031] And since a location (current position) and time amount (current time) are acquired automatically, they are less necessary, and can simplify time and effort. [of a user's information management] Moreover, it is physically impossible to carry out decode processing to the time amount as which specific accepting-station equipment was specified by two or more places, and probability for information to be decoded can be made lower.

[0032] (5) In the explanation beyond the modification of an operation gestalt, as an encryption key, although the location encryption key, the time amount encryption key, and the user specification encryption key were used, it is also possible to combine the encryption key of arbitration and the password of arbitration further. In the above-mentioned explanation, although the case where positional information and a hour entry were used as an encryption key was explained, it is also possible to constitute so that it may process by using these one side or both sides as a password, and may constitute or may process as a password and an encryption key.

[0033] Moreover, in the above-mentioned explanation, although GPS using a GPS Satellite was used as a self-location detection means, it is also possible to constitute so that the information which pinpoints a base transceiver station may be used like the enclosure of PHS in using the false GPS information by the false GPS Satellite (GPS electric wave transmitter) installed suitably and the location registration information in PHS etc. Thereby, a self-location is detectable per two or more wireless zone unit or room.

[0034] Moreover, as a cipher system, you may be which method of a common key system or a public key system. For example, a common key is generable by combining the location encryption key (indispensable) mentioned above, a time amount encryption key (arbitration), a transmitting person's public key, and an addressee's E mail address by the predetermined operation in the case of a common key system. In the above explanation, although the case of an electronic mail system was explained, if it is data in which not only electronic mail data but electronization is possible, it is applicable. For example, about sensitive data, if it is not a specific location in the company, when perusal etc. is made to be not possible, read-out of the data by personnel without authority etc. can be prevented.

[0035]

[Effect of the Invention] According to this invention, it becomes possible by enciphering using positional information and a hour entry at least to raise the protection to an informational theft or tapping and to raise confidentiality. Moreover, the burden of the user for information management is not made to increase by acquiring positional information and a hour entry automatically. Furthermore, since it is physically impossible, trying decode processing by two or more places to the time amount as which one equipment was specified can make lower probability for information to be decoded.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1] It is an outline block diagram at the time of building a code electronic mail system.
[Drawing 2] It is outline configuration block drawing of accepting-station equipment.
[Drawing 3] It is functional configuration block drawing of a code electronic mail system.
[Drawing 4] It is the processing sequence diagram of a code electronic mail system.
[Drawing 5] It is drawing explaining the example of a data configuration in the condition data base section.
[Description of Notations]
10 — Code electronic mail system,
11 — Encryption server,
12 — Mail server,
13 — Radio relay station,
14 — Network,
15 — Transmit-terminal equipment,
20 — Accepting-station equipment (pocket mold information processor),
21 — CPU,
22 — Memory,
23 — Display,
24 — Input unit,
25 — External storage,
26 — Antenna for transmitters,
27 — Data communication unit
28 — GPS receiving antenna,
29 — GPS receiver
30 — Computer for GPS,
31 — Loudspeaker,
32 — Extended bus interface,
33 — Internal bus

[Translation done.]

* NOTICES *

Japan Patent Office is not responsible for any damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1] Encryption equipment characterized by having an encryption key generation means to generate an encryption key, and an encryption means to encipher input using said encryption key, using inputted positional information and inputted time information.
[Claim 2] It is encryption equipment characterized by generating said encryption key using transmission place specific information for said encryption key generation means specifying a transmission place of said input in encryption equipment according to claim 1 in addition to said positional information and said time information.
[Claim 3] Decryption equipment characterized by having a decryption key generation means to generate a decryption key using inputted currency information and inputted current time information, and a decryption means to decrypt input encryption information using said decryption key.
[Claim 4] It is decryption equipment characterized by generating said decryption key using transmission place specific information for said decryption key generation means specifying a transmission place of said input encryption information in decryption equipment according to claim 3 in addition to said currency information and said current time information.
[Claim 5] The pocket information processor carry out having had a self-location detection means detects the self current position and output currency information in the pocket information processor which decrypts the input encryption information which is inputted encryption data, the current-time detection means detect current time and output current-time information, the decryption key generation means generate a decryption key using said currency information and said current-time information, and the decryption means decrypt input encryption information using said decryption key as the feature.
[Claim 6] Encryption equipment characterized by having an encryption key generation processing circuit which generates an encryption key, and an encryption processing circuit which enciphers input using said encryption key using inputted positional information and inputted time information.
[Claim 7] Encryption equipment characterized by having a decryption key generation processing circuit which generates a decryption key using inputted currency information and inputted current time information, and a decryption processing circuit which decrypts input encryption information using said decryption key.
[Claim 8] A pocket information processor which decrypts input encryption information which is characterized by providing the following, and which is inputted encryption data Self-location detection equipment which detects the self current position and outputs currency information Current time detection equipment which detects current time and outputs current time information A decryption key generation processing circuit which generates a decryption key using said currency information and said current time information A decryption processing circuit which decrypts input encryption information using said decryption key
[Claim 9] An encryption method characterized by having an encryption key generation production process which generates an encryption key, and an encryption production process which enciphers input using said encryption key using inputted positional information and

inputted time information.
[Claim 10] A decryption method characterized by having a decryption key generation production process which generates a decryption key using inputted currency information and inputted current time information, and a decryption production process which decrypts input encryption information using said decryption key.
[Claim 11] A control method of a pocket information processor which decrypts input encryption information which is characterized by providing the following, and which is inputted encryption data A self-location detection production process of detecting the self current position A current time detection production process of detecting current time A decryption key generation production process which generates a decryption key using said detected current position and said detected current time A decryption production process which decrypts encryption information inputted using said generated decryption key

---

[Translation done.]